

ICS 35.030

GM

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GM/T 0118-2022

Browser digital certificate application interface specification

浏览器数字证书应用接口规范

(English Translation)

Issued on: November 20, 2022

Implemented on: June 1, 2023

Issued by: State Administration of Cryptography

Table of Contents

Foreword	1
Scope	2
Normative references	3
Terms and definitions	4
Abbreviations	5
Overall technical framework	6
Algorithm identification	7
Overview	8
Create certificate context	9
Add certificate to certificate storage	10
Find CRL in the certificate store	11
Traverse CRL in the certificate store	12
Relationship with other interface specifications	13
Foreword	14
Overview	15
Create certificate context	16
Add certificate to certificate storage	17
Find CRL in the certificate store	18
Traverse CRL in the certificate store	19
Relationship with other interface specifications	20

Foreword

This document was drafted in accordance with the provisions of GB/T 1.1-2020 "Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents".

Please note that some contents of this document may involve patents. The issuing agency of this document does not assume the responsibility for identifying patents.

This document was proposed by AND shall be under the jurisdiction of the Technical Committee for Standardization of the Cryptography Industry.

Drafting organizations of this document. Tianjin Yingdaxin Technology Co., Ltd., Beijing Xin'an Century Technology Co., Ltd., Beijing Digital Certification Co., Ltd., Beijing Hitech

Fangyuan Technology Co., Ltd., China Minsheng Bank Co., Ltd., Beijing Qihoo Technology Co., Ltd., Asia Information Technology (Shanghai) Co., Ltd.

1 Scope

This document specifies the browser SM2 digital certificate application interface;

describes the definition of functions, data types and parameters of the digital certificate application interface in browsers, that support the application of domestic cryptographic algorithms.

This document is applicable to the development, application, testing of browser products, the development of browser applications that support SM2 digital certificates, the testing of secure browser password modules; it can also be used to guide the integration and development of third-party applications calling SM2 digital certificates in different terminal devices.

2 Normative references

The contents of the following documents constitute essential clauses of this document through normative references in the text. Among them, for dated references, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies to this document.

GB/T 20518 Information security technology - Public key infrastructure - Digital certificate format
GB/T 32918.2 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 2: Digital signature algorithm
GB/T 33560 Information security technology - Cryptographic application identifier criterion specification

3 Terms and definitions

The terms and definitions as defined in GM/Z 4001, as well as the following terms and definitions, apply to this document.

SM2 cryptographic algorithm Public key cryptographic algorithm defined by GB/T 32918.5.

Digital certificate

Also known as public key certificate, which is a data structure signed by a certificate authority (CA) that contains public key owner information, public key, issuer information, validity period, extended information. It can be divided into personal certificate, agency certificate, device certificate by type; or it can be divided into signature certificate and encryption certificate by purpose.

Digital signature

The result obtained by the signer using the private key to perform cryptographic operations

on the signed data. The result can only be verified by the signer's public key and is used to confirm the integrity of the data to be signed, the authenticity of the signer's identity, the non-repudiation of the signature behavior.

Certificate context

A data structure, which is used to store relevant certificate information, including owner information, public key, issuer information, validity period, extended information.

4 Abbreviations

The following abbreviations apply to this document.

AIA. Authority Information Access API. Application Programming Interface CRL. Certificate Revocation List

5 Overall technical framework

The overall technical framework of the browser digital certificate application interface is shown in Figure 1.

6.1 Algorithm identification

The identification definition of the algorithm used in this document is implemented in accordance with GB/T 33560.

7.1 Overview

The algorithm used in this document shall comply with GB/T 33560 in its identification definition; the error code shall comply with the provisions of Appendix A.

The browser digital certificate application interface standard mainly consists of the following parts.

7.2.1 Create certificate context

Function prototype.

7.2.3 Add certificate to certificate storage

Function prototype

7.2.14 Find CRL in the certificate store

Function prototype.

7.2.15 Traverse CRL in the certificate store

Function prototype.

Function description. Traverse CRL in the certificate store. Call this function to obtain the CRL linked list and eventually all CRLs.

7.5 Relationship with other interface specifications

For GM/T 0019, its main purpose is to provide general cryptographic services such as certificate parsing, certificate authentication, confidentiality, integrity and non-repudiation of information to the cryptographic service layer and application layer, through a unified cryptographic service interface;

GM/T 0118-2022

CRYPTOGRAPHIC INDUSTRY STANDARD ICS 35.030 L 80 Browser digital certificate application interface specification Issued on. NOVEMBER 20, 2022 Implemented on. JUNE 01, 2023 Issued by. State Cryptography Administration

Table of Contents

Foreword...	3
1 Scope...	4
2 Normative references...	4
3 Terms and definitions...	5
4 Abbreviations...	6
5 Overall technical framework...	6
6 Algorithm identification and data type...	7
6.1 Algorithm identification...	7
6.2 Basic data types...	7
6.3 Constant definition...	8
6.4 Composite data type...	9
7 Interface function...	18
7.1 Overview...	18
7.2 Certificate storage area management interface...	20
7.3 UI interface...	28
7.4 SKF management interface...	30